PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2003-198539**
(43)Date of publication of application : **11.07.2003**

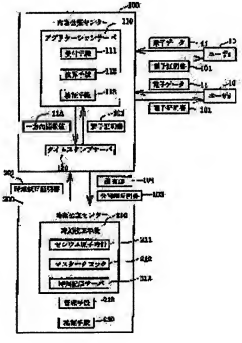
(51)Int.Cl. **H04L 9/32**
G06F 17/60
G09C 1/00

(21)Application number : **2001-396856**
(22)Date of filing : **27.12.2001**

(71)Applicant : **SEIKO INSTRUMENTS INC**
(72)Inventor : **MIYAHARA SHINICHIRO**
SHIBATA KOICHI

(54) ELECTRONIC AUTHENTICATION SYSTEM AND ELECTRONIC AUTHENTICATION METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an electronic authentication system and an electronic authentication method in which reliability of time stamp information is improved.
SOLUTION: The system is provided with a contents authentication center 100 for receiving the registration of electronic information for a user, issuing an electronic certificate 101 and verifying contents on the basis of the relevant electronic certificate 101 and an independent time authentication center 200 for verifying a time on the basis of the electronic certificate 101. The contents authentication center 100 prepares the electronic certificate 101 by using a time-corrected time stamp means 120 and the time authentication center 20 is provided with a management means 220 for storing information of a public key paired with a secret key to be intrinsically used by the time stamp means 120 together with the ID of the relevant time stamp means 120 and a time verifying means 230 for receiving a verification request based on the electronic certificate 101 from the user and verifying the time on the basis of the information stored in the management means 220.



LEGAL STATUS

[Date of request for examination]	09.10.2002
[Date of sending the examiner s decision of rejection]	
[Kind of final disposal of application other than the examiner s decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3717848
[Date of registration]	09.09.2005
[Number of appeal against examiner s decision of rejection]	
[Date of requesting appeal against examiner s decision of rejection]	
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－198539
（Ｐ2003－198539Ａ）
(43)公開日　平成15年７月11日(2003.7.11)

(51)Int.Cl.⁷	識別記号	ＦＩ		ﾃｰﾏｺｰﾄﾞ(参考)
Ｈ04Ｌ　9/32		Ｃ06Ｆ　17/60	140	5Ｊ104
Ｇ06Ｆ　17/60	140		512	
	512		ZEC	
	ZEC	Ｇ09Ｃ　1/00	640D	
Ｇ09Ｃ　1/00	640	Ｈ04Ｌ　9/00	675D	

審査請求 有　請求項の数10　ＯＬ　（全９頁）　最終頁に続く

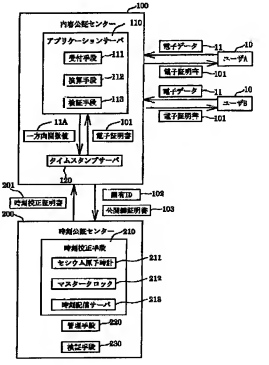
(21)出願番号　特願2001－396856(Ｐ2001－396856)
(22)出願日　平成13年12月27日(2001.12.27)

(71)出願人　000002325
セイコーインスツルメンツ株式会社
千葉県千葉市美浜区中瀬１丁目８番地
(72)発明者　宮原　慎一郎
千葉県千葉市美浜区中瀬１丁目８番地　セイコーインスツルメンツ株式会社内
(72)発明者　柴田　孝一
千葉県千葉市美浜区中瀬１丁目８番地　セイコーインスツルメンツ株式会社内
(74)代理人　100096378
弁理士　坂上　正明

Ｆターム(参考)　5Ｊ104 AA08 EA19 LA01 LA03 LA06 MA03 PA07

(54)【発明の名称】　電子公証システム及び電子公証方法

(57)【要約】　（修正有）
【課題】　タイムスタンプ情報の信頼性を向上させた電子公証システム及び電子公証方法を提供する。
【解決手段】　利用者から電子情報の登録を受け付けて電子証明書１０１を発行すると共に当該電子証明書１０１に基づいて内容検証を行う内容公証センター１００と、前記電子証明書１０１に基づいて時刻検証を行う独立の時刻公証センター２００とを具備する。前記内容公証センター１００は、時刻校正されたタイムスタンプ手段１２０を用いて前記電子証明書１０１を作成し、前記時刻公証センター２００は、時刻校正手段２１０と、前記タイムスタンプ手段１２０が固有に使用する秘密鍵と対をなす公開鍵に関する情報を当該タイムスタンプ手段１２０のＩＤと共に蓄積する管理手段２２０と、利用者からの前記電子証明書１０１に基づいた検証要求を受け付けて前記管理手段２２０が蓄積した情報に基づいて時刻検証を行う時刻検証手段２３０とを具備する。



【特許請求の範囲】
【請求項１】　ネットワーク上において電子公証を行う電子公証システムにおいて、
利用者から電子情報の登録を受け付けて電子証明書を発行すると共に当該電子証明書に基づいて内容検証を行う内容公証センターと、前記内容公証センターとは独立して存在して前記電子証明書に基づいて時刻検証を行う時刻公証センターとを具備し、
前記内容公証センターは、前記時刻公証センターが時刻校正するタイムスタンプ手段を用いて前記電子証明書を作成し、前記時刻公証センターは、前記タイムスタンプ手段の時刻校正を行う時刻校正手段と、前記タイムスタンプ手段が固有に使用する秘密鍵と対をなす公開鍵の情報若しくは当該公開鍵を特定するための情報であって前記電子証明書に含まれる特定情報を当該タイムスタンプ手段のＩＤと共に蓄積する管理手段と、利用者からの前記電子証明書に基づいた検証要求を受け付けて前記管理手段が蓄積した情報に基づいて時刻検証を行う時刻検証手段とを具備することを特徴とする電子公証システム。
【請求項２】　前記管理手段は、ネットワークを介して前記タイムスタンプ手段にアクセスして当該タイムスタンプ手段のＩＤ及び前記特定情報を取得することを特徴とする請求項１に記載の電子公証システム。
【請求項３】　前記管理手段は、前記時刻校正手段が前記タイムスタンプ手段の時刻校正を行う際に前記特定情報を取得することを特徴とする請求項１又は２に記載の電子公証システム。
【請求項４】　前記時刻校正手段は、時刻校正を行う際に時刻校正証明書を前記タイムスタンプ手段に送信し、当該タイプスタンプ手段は、この時刻校正証明書を含めて前記電子証明書を発行することを特徴とする請求項１～３の何れかに記載の電子公証システム。
【請求項５】　前記特定情報は、前記タイムスタンプ手段が使用する秘密鍵と対をなす公開鍵の公開鍵証明書であることを特徴とする請求項１～４の何れかに記載の電子公証システム。
【請求項６】　ネットワーク上において電子公証を行う電子公証方法において、
利用者から電子情報の登録を受け付けて電子証明書を発行すると共に当該電子証明書に基づいて内容検証を行う内容公証センターと、前記内容公証センターとは独立して存在して前記電子証明書に基づいて時刻検証を行う時刻公証センターとを設け、
前記内容公証センターは、前記時刻公証センターが時刻校正するタイムスタンプ手段を用いて前記電子証明書を作成する一方、前記時刻公証センターは、前記タイムスタンプ手段の時刻校正を行うと共に、前記タイムスタンプ手段が固有に使用する秘密鍵と対をなす公開鍵の情報若しくは当該公開鍵を特定するための情報であって前記電子証明書に含まれる特定情報を当該タイムスタンプ手段のＩＤと共に蓄積し、この蓄積情報に基づき、利用者からの前記電子証明書に基づいた検証要求に応じて時刻検証を行うことを特徴とする電子公証方法。
【請求項７】　前記時刻校正センターは、ネットワークを介して前記タイムスタンプ手段にアクセスして当該タイムスタンプ手段のＩＤ及び前記特定情報を取得することを特徴とする請求項６に記載の電子公証方法。
【請求項８】　前記時刻校正センターは、前記タイムスタンプ手段の時刻校正を行う際に前記特定情報を取得することを特徴とする請求項６又は７に記載の電子公証方法。
【請求項９】　前記時刻校正センターは、時刻校正を行う際に時刻校正証明書を前記タイムスタンプ手段に送信し、当該タイプスタンプ手段は、この時刻校正証明書を含めて前記電子証明書を発行することを特徴とする請求項６～８の何れかに記載の電子公証方法。
【請求項１０】　前記特定情報は、前記タイムスタンプ手段が使用する秘密鍵と対をなす公開鍵の公開鍵証明書であることを特徴とする請求項６～９の何れかに記載の電子公証方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、電子公証システム及び電子公証方法に関する。
【０００２】
【従来の技術】インターネットの普及により、インターネットを介してショッピングや取引を行う電子商取引が一般化され、また、インターネット上で契約を行う必要性が出てきた。
【０００３】そこで、電子ネットワーク上で安心して電子商取引や契約を行うことができるために、電子ネットワーク上で公証を行う電子公証システムが出現した。
【０００４】電子公証システムは、電子情報について、「いつ、誰が、何を」を登録、照会、証明するシステムである。したがって、電子ネットワーク上の通信を安全に行うための暗号化技術、公開鍵暗号方式を使用した電子署名技術及び正確な時刻を証明するタイムスタンプ技術が必要となる。
【０００５】従来の電子公証システムは、図５に示すように行われる。電子公証サービス事業者１は、利用者であるＡ社２及びＢ社３等に対して電子公証サービスを提供する、例えば、Ａ社２から電子文書４の登録を受け付け、それに対して電子証明書５を発行する。電子証明書５は、電子文書４の内容から一方向関数によって出力される一方向関数値、例えば、ハッシュ値、時刻情報およびそれらに対しての電子署名等を含むものである。利用者であるＡ社２とＢ社３とが電子文書４及び電子証明書５を使用して電子商取引を行う際に、Ｂ社３が電子文書４及び電子証明書５を電子公証サービス事業者１へ送信することにより照会を行うと、電子公証サービス事業１

は電子文書4及び電子証明書5の検証を行い、結果をB社3へ通知する。

【0006】

【発明が解決しようとする課題】上述したような電子公証システムでは、電子文書4が登録された時間を証明する電子証明書5に含まれる時間情報が正確な時刻であるかどうかについて、疑義が生じる可能性がある。すなわち、正確な時刻をタイムスタンプされているか？改ざんされた時刻ではないか？などの疑問が生じるという問題がある。

【0007】本発明は、このような事情に鑑み、タイムスタンプ情報の信頼性を向上させた電子公証システム及び電子公証方法を提供することを課題とする。

【0008】

【課題を解決するための手段】前記課題を解決する本発明の第1の態様は、ネットワーク上において電子公証を行う電子公証システムにおいて、利用者から電子情報の登録を受け付けて電子証明書を発行すると共に当該電子証明書に基づいて内容検証を行う内容公証センターと、前記内容公証センターとは独立して存在して前記電子証明書に基づいて時刻検証を行う時刻公証センターとを具備し、前記内容公証センターは、前記時刻公証センターが時刻校正するタイムスタンプ手段を用いて前記電子証明書を作成し、前記時刻公証センターは、前記タイムスタンプ手段の時刻校正を行う時刻校正手段と、前記タイムスタンプ手段が固有に使用する秘密鍵と対をなす公開鍵の情報若しくは当該公開鍵を特定するための情報であって前記電子証明書に含まれる特定情報を当該タイムスタンプ手段のＩＤと共に蓄積する管理手段と、利用者からの前記電子証明書に基づいた検証要求を受け付けて前記管理手段が蓄積した情報に基づいて時刻検証を行う時刻検証手段とを具備することを特徴とする電子公証システムにある。

【0009】本発明の第2の態様は、第1の態様において、前記管理手段は、ネットワークを介して前記タイムスタンプ手段にアクセスして当該タイムスタンプ手段のＩＤ及び前記特定情報を取得することを特徴とする電子公証システムにある。

【0010】本発明の第3の態様は、第1又は2の態様において、前記管理手段は、前記時刻校正手段が前記タイムスタンプ手段の時刻校正を行う際に前記特定情報を取得することを特徴とする電子公証システムにある。

【0011】本発明の第4の態様は、第1～3の何れかの態様において、前記時刻校正手段は、時刻校正を行う際に時刻校正証明書を前記タイムスタンプ手段に送信し、当該タイプスタンプ手段は、この時刻校正証明書を含めて前記電子証明書を発行することを特徴とする電子公証システムにある。

【0012】本発明の第5の態様は、第1～4の何れかの態様において、前記特定情報は、前記タイムスタンプ手段が使用する秘密鍵と対をなす公開鍵の公開鍵証明書であることを特徴とする電子公証システムにある。

【0013】本発明の第6の態様は、ネットワーク上において電子公証を行う電子公証方法において、利用者から電子情報の登録を受け付けて電子証明書を発行すると共に当該電子証明書に基づいて内容検証を行う内容公証センターと、前記内容公証センターとは独立して存在して前記電子証明書に基づいて時刻検証を行う時刻公証センターとを設け、前記内容公証センターは、前記時刻公証センターが時刻校正するタイムスタンプ手段を用いて前記電子証明書を作成する一方、前記時刻公証センターは、前記タイムスタンプ手段の時刻校正を行うと共に、前記タイムスタンプ手段が固有に使用する秘密鍵と対をなす公開鍵の情報若しくは当該公開鍵を特定するための情報であって前記電子証明書に含まれる特定情報を当該タイムスタンプ手段のＩＤと共に蓄積し、この蓄積情報に基づき、利用者からの前記電子証明書に基づいた検証要求に応じて時刻検証を行うことを特徴とする電子公証方法にある。

【0014】本発明の第7の態様は、第6の態様において、前記時刻校正センターは、ネットワークを介して前記タイムスタンプ手段にアクセスして当該タイムスタンプ手段のＩＤ及び前記特定情報を取得することを特徴とする電子公証方法にある。

【0015】本発明の第8の態様は、第6又は7の態様において、前記時刻校正センターは、前記タイムスタンプ手段の時刻校正を行う際に前記特定情報を取得することを特徴とする電子公証方法にある。

【0016】本発明の第9の態様は、第6～8の何れかの態様において、前記時刻校正センターは、時刻校正を行う際に時刻校正証明書を前記タイムスタンプ手段に送信し、当該タイプスタンプ手段は、この時刻校正証明書を含めて前記電子証明書を発行することを特徴とする電子公証方法にある。

【0017】本発明の第10の態様は、第6～9の何れかの態様において、前記特定情報は、前記タイムスタンプ手段が使用する秘密鍵と対をなす公開鍵の公開鍵証明書であることを特徴とする電子公証方法にある。

【0018】かかる本発明では、電子情報についての電子証明書に基づいて内容検証を行う内容公証センターと、電子証明書に基づいて時刻検証を行う時刻公証センターとを独立させることにより、正確な時刻をタイムスタンプされているか？改ざんされた時刻ではないか？などの疑問が生じることなく、タイムスタンプ情報の信頼性を向上させることができる。

【0019】

【発明の実施の形態】以下、本発明の実施の形態について、図面を参照して詳細に説明する。

【0020】図1には、一実施形態に係る電子データ公証システムの概要を示す。同図に示すように、本実施形

態の電子データ公証システムは、内容公証センター１００及び時刻公証センター２００が対となって電子データの内容及び時刻の公証サービスをユーザA、ユーザB等のユーザ１０に提供するものであり、一つの時刻公証センター２００に対して複数の内容公証センター１００が存在し、サービスを提供することができる。なお、内容公証センター１００及び時刻公証センター２００とは、相互に独立した主体が管理するのが好ましい。また、各ユーザ１０は、名称又は氏名、固有ＩＤの他、電子署名および署名に用いる公開鍵証明書等を、事前に内容公証センター１００及び時刻公証センター２００へ登録するのが好ましい。これにより、公証をスムーズに行うことができ、また、ユーザ１０と内容公証センター１００との通信を全て署名・暗号化して行うことができ、通信段階での改ざん、盗聴、成りすまし等を防止することができる。

【００２１】ここで、ユーザ１０は、電子データ１１を内容公証センター１００へ送信することにより、その電子データ１１の内容及び時刻を公証するための電子証明書１０１を受信することができる。なお、ユーザ１０は、好ましくは、予め、内容公証センター１００に登録した電子署名を用いて電子データ１１を暗号化して送信するようにするのが好ましい。

【００２２】一方、内容公証センター１００は、ユーザ１０から公証の受付及び検証を行うアプリケーションサーバ１１０を有し、アプリケーションサーバ１１０は、ユーザ１０からの受付及びユーザ１０への電子証明書１０１の送信を行う受付手段１１１と、受け付けた電子データ１１を受信して電子証明書１０１を作成するための一方向関数値を作成する演算手段１１２と、ユーザ１０からの検証要求に対応する検証手段１１３とを具備する。また、内容公証センター１００は、一方向関数値にタイムスタンプ情報を付与して電子証明書１０１を発行するタイムスタンプサーバ１２０を具備する。

【００２３】ここで、受付手段１１１は、ユーザ１０からの接続要求を受け付け、ユーザ１０の固有ＩＤなどの必要な情報を受信すると共に、電子データ１１を受信する。なお、電子データ１１が暗号化されている場合には、復号すると共に電子署名により改ざん等が無いことを検証する。

【００２４】演算手段１１２は、受付手段１１１が受信した電子データ１１から一方向関数値を作成し、タイムスタンプサーバ１２０に渡す。ここで、一方向関数値とは、例えば、ハッシュ（ＨＡＳＨ）値、メッセージダイジェストとも呼ばれるもので、ハッシュ関数などの不可逆な一方向関数により生成された、例えば、固定長の疑似乱数である。同一のデータからは同一の一方向関数値が得られるが、一方向関数値から元のデータを再現することはできない。

【００２５】検証手段１１３は、ユーザ１０からの電子データ１１及びそれに対する電子証明書１０１と共に検証要求を受け付け、これらに対する改ざん等がないことを検証するもので、詳細は後述する。

【００２６】タイムスタンプサーバ１２０は、演算手段１１２から一方向関数値を受け取り、これにタイムスタンプ情報を付加して電子証明書１０１を作成するものであれば特に限定されない。また、電子証明書１０１は、所定の手順により暗号化・署名されているのが好ましく、タイムスタンプサーバ１２０により使用される時刻情報は、時刻公証センター２００により定期的に校正されている。なお、これらの点に付いて詳細は後述する。

【００２７】タイムスタンプサーバ１２０の時刻校正を行う時刻公証センター２００は、時刻校正手段２１０を具備し、時刻校正手段２１０は、例えば、協定世界時と協調するセシウム原子時計２１１、セシウム原子時計２１１から時刻ソースが供給されるマスタークロック２１２及びマスタークロック２１２から時刻配信される時刻配信サーバ２１３とを具備し、時刻配信サーバ２１３がタイムスタンプサーバ１２０の時刻手段を定期的に校正する。

【００２８】ここで、時刻公証センター２００は、定期的にタイムスタンプサーバ１２０にアクセスし、内蔵される時計の校正を行うと共に、タイムスタンプサーバ１２０の固有ＩＤ１０２及び当該タイムスタンプサーバ１２０が使用する公開鍵の公開鍵証明書１０３を取得し、当該公開鍵証明書１０３の一方向関数値であるハッシュ値を含む時刻校正証明書２０１を発行する。

【００２９】また、時刻公証センター２００は、各タイムスタンプサーバ１２０の固有ＩＤ１０２と共に当該タイムスタンプサーバ１２０が使用する公開鍵を特定する情報を蓄積して管理する管理手段２２０と、ユーザ１０からの電子データ１１及びそれに対する電子証明書１０１と共に検証要求を受け付け、これらに対する改ざん等がないことを検証する検証手段２３０とを具備する。ここで、タイムスタンプサーバ１２０が使用する公開鍵を特定する特定情報としては、時刻校正手段２１０がタイムスタンプサーバ１２０の時刻公証を行う際に取得する公開鍵証明書１０３を挙げることができるが、これに限定されず、タイムスタンプサーバ１２０が使用する公開鍵を別途取得して蓄積してもよい。

【００３０】このようなタイムスタンプサーバ１２０の一例及びこのタイムスタンプサーバ１２０により発行される電子証明書１０１の一例を図２に示す。図２に示すように、タイムスタンプサーバ１２０は、時刻公証センター２００により管理された固有ＩＤ１０２を有すると共に時計１２１を内蔵し、電子証明書作成手段１２２を具備する。また、電子証明書１０１を作成する際に暗号化に使用する秘密鍵１２３及びこの秘密鍵１２３と対をなす公開鍵の公開鍵証明書１０３を有する。また、タイムスタンプサーバ１２０の時計１２１は、上述したよう

に、時刻公証センター２００の時刻校正手段２１０により定期的に所定のタイミングで校正されており、この校正時に時刻校正証明書２０１を受信し、これを保管している。なお、時刻公証センター２００は、時刻校正時にタイムスタンプサーバ１２０から固有ＩＤ１０２及び公開鍵証明書１０３を取得し、これにより、当該タイムスタンプサーバ１２０が適正な電子証明書１０１を生成しているかどうかを監視し、発行した電子証明書１０１について認証する。

【００３１】電子証明書作成手段１２２は、ユーザ１０の電子データ１１の一方向関数値１１Ａを演算手段１１２から受信してこれに時計１２１から取得した時刻情報を付加したタイムスタンプ情報１０４を作成すると共に、このタイムスタンプ情報１０４を秘密鍵１２３で暗号化すると共に署名した電子署名１０５を作成し、電子証明書１０１として出力する。従って、電子証明書１０１は、タイムスタンプ情報１０４及び電子署名１０５を具備し、さらに、タイムスタンプ用秘密鍵の公開鍵証明書１０３及び時刻校正証明書２０１を含むものである。

【００３２】このような電子証明書１０１の使用例を図３に示す。図３に示す例では、電子証明書１０１を内容公証センター１００から取得したユーザ１０（ユーザＡ）が、電子データ１１と共に電子証明書１０１をユーザ２０（ユーザＸ）に対して使用し、ユーザ２０が電子データ１１及び電子証明書１０１を使用して内容検証要求３０１を行う場合を想定している。ここで、ユーザ２０は、電子データ１１及び電子証明書１０１を用いて内容公証センター１００へ内容検証要求３０１を行うことにより、電子データ１１の改ざん、日付の変更等がないことを内容証明３０２により確認をすることができる。一方、ユーザ２０は、電子証明書１０１を用いて時刻公証センター２００へ時刻検証要求３０３を行うことにより、内容公証センター１００が時刻公証センター２００による時刻校正を受けている正規のタイムスタンプサーバ１２０を使用しており、電子証明書１０１が正規のタイムスタンプサーバ１２０が発行したものであることを、時刻証明３０４により確認することができる。すなわち、ユーザ２０は、電子情報のやりとりだけで、電子情報の改ざん等による不正を看破することができる。

【００３３】ここで、内容公証センター１００が内容証明３０２を行う手段、並びに時刻公証サーバ２００が時刻証明３０４を行う手段については特に限定されず、ユーザ２０に対して証明書を発行してもよいし、電子メール等で連絡してもよいし、ユーザ２０がウェブ上で確認できるようにしてもよい。

【００３４】また、内容公証センター１００は、検証手段１１３が、例えば、ユーザ２０から受信した電子データ１１から上述した演算手段１１２と同様にハッシュ値を求め、これと、電子証明書１０１のタイムスタンプ情報１０４に含まれるハッシュ値と一致するかどうかを検証することにより、内容証明３０２を行う。勿論、検証手段１１３は、電子データ１１の内容のみの検証ではなく、すなわち、内容に改ざん等があるか否かの検証だけでなく、タイムスタンプ情報に改ざん等があるか否かの検証をも行うものである。

【００３５】一方、時刻公証センター２００の検証手段２３０が時刻証明３０４を行うまでの手順は図４に示す通りである。すなわち、ユーザ２０から電子証明書１０１と共に時刻検証要求３０３を受けると、受信した電子証明書１０１のタイムスタンプ情報１０４に含まれているタイムスタンプサーバ１２０の固有ＩＤ１０２と、時刻校正証明書２０１を作成した際に使用した公開鍵証明書１０３とを含む検証情報１０６を取得する。この検証情報１０６が、管理手段２２０が蓄積した固有ＩＤ１０２及び公開鍵証明書１０３を含むデータベース２２１に含まれるか否かを検証し、含まれることを条件として時刻証明３０４を行う。ここで、時刻証明３０４は、内容証明３０２のように電子証明書１０１に改ざん、不正があるか否かではなく、電子証明書１０１が、時刻公証センター２００により所定の時刻校正を受けて管理されているタイムスタンプサーバ１２０により発行された真正なものであることを証明するものである。

【００３６】通常、時刻校正証明書２０１が真正なものかどうかを検証することにより、電子証明書１０１を真正なものとみなすことができるが、時刻校正証明書２０１自体を模倣・複写することも考えられるので、タイムスタンプ情報１０４に含まれる固有ＩＤ１０２と時刻校正証明書２０１を作成した際に使用した公開鍵証明書１０３との対により、正規のタイムスタンプサーバ１２０が発行したものか否かを検証するようにしている。また、時刻校正証明書２０１を検証することにより、当該電子証明書１０１を発行したタイムスタンプサーバ１２０が現在でも定期的に時刻校正を受けているかを把握することができ、これにより、電子証明書１０１に含まれるタイムスタンプ情報１０４が正確か否かの判断を行うことができる。さらに、このような検証を行うことにより、偽の固有ＩＤ及び公開鍵証明書を保有した偽のタイムスタンプサーバが発行した電子証明書も看破することができる。

【００３７】以上説明したように、電子情報についての電子証明書に基づいて内容検証を行う内容公証センターと、電子証明書に基づいて時刻検証を行う時刻公証センターとを独立させることにより、時刻検証については必要に応じて二重に検証することができ、タイムスタンプ情報の信頼性を向上させることができるので、タイムスタンプ情報が重視された新しい使用態様に対応することができる。

【００３８】

【発明の効果】本発明によれば、電子情報についての電子証明書に基づいて内容検証を行う内容公証センター

と、電子証明書に基づいて時刻検証を行う時刻公証センターとを独立させることにより、正確な時刻をタイムスタンプされているか？改ざんされた時刻ではないか？などの疑問が生じることなく、タイムスタンプ情報の信頼性を向上させることができるという効果を奏する。

【図面の簡単な説明】

【図１】本発明の一実施形態に係る電子データ公証システムの概略構成例を示す図である。

【図２】本発明の一実施形態におけるタイムスタンプサーバ及び電子証明書を説明する図である。

【図３】本発明の一実施形態における電子証明書の使用態様を表す図である。

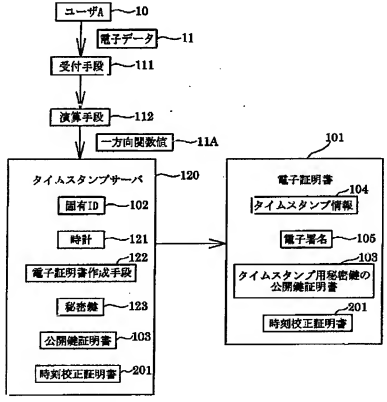
【図４】本発明の一実施形態に係る時刻証明の手順を説明する図である。

【図５】従来技術に係る電子公証システムの概略構成例を示す図である。

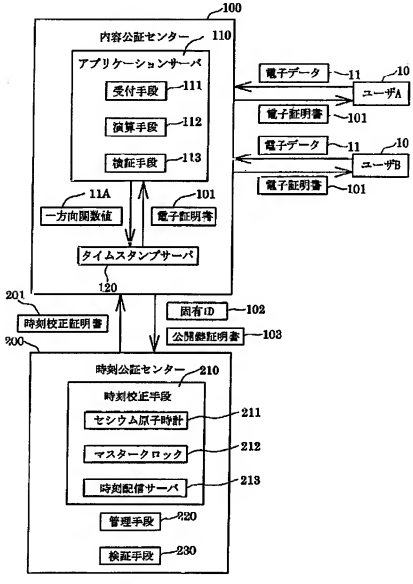
【符号の説明】

１０　ユーザA、ユーザB
２０　ユーザX
１１　電子データ
１１A　一方向関数値
１００　内容公証センター
１０１　電子証明書
１０２　固有ＩＤ
１０３　公開鍵証明書
１１０　アプリケーションサーバ
１１１　受付手段
１１２　演算手段
１１３　検証手段
１２０　タイムスタンプサーバ
２００　時刻公証センター
２１０　時刻校正手段
２２０　管理手段
２３０　検証手段

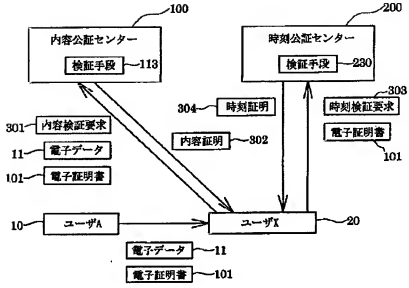
【図２】



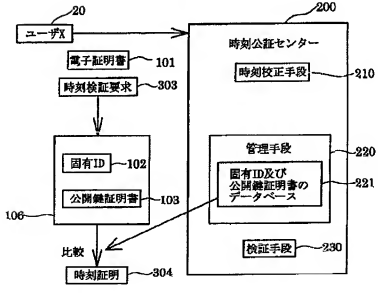
【図1】


100
内容公証センター
110
アプリケーションサーバ
受付手段
111
演算手段
112
検証手段
113
11A
一方向関数値
101
電子証明書
タイムスタンプサーバ
120
電子データ
11
10
ユーザA
電子証明書
101
電子データ
11
10
ユーザB
電子証明書
101
201
時刻校正証明書
固有ID
102
公開鍵証明書
103
200
時刻公証センター
210
時刻校正手段
セシウム原子時計
211
マスタークロック
212
時刻配信サーバ
213
管理手段
220
検証手段
230

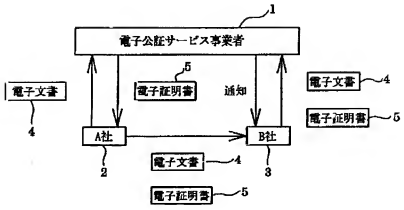
【図３】


100
内容公証センター
検証手段
113
200
時刻公証センター
検証手段
230
303
時刻検証要求
304
時刻証明
301
内容検証要求
内容証明
302
電子証明書
101
11
電子データ
101
電子証明書
10
ユーザA
ユーザX
20
電子データ
11
電子証明書
101

【図４】


20
ユーザX
200
時刻公証センター
電子証明書
101
時刻校正手段
210
時刻検証要求
303
管理手段
220
固有ID
102
固有ID及び
公開鍵証明書の
データベース
221
公開鍵証明書
103
106
比較
検証手段
230
時刻証明
304

【図5】



フロントページの続き

(51)Int.Cl.[7]	識別記号	FI	(参考)
		H04L 9/00	675B